U.S. Application No. 09/685,026   2
Docket No. YOR920000165US1
(YOR.203)

AMENDMENTS TO THE CLAIMS:

1.   (Currently amended) A method of preventing counterfeiting of a smart card,

comprising:

providing a smart card with a cryptographic structure for authorizing the smart card

which cannot be accessed completely by a predetermined small number of readings,

wherein said cryptographic structure can be built only by whoever emits the

card or an agent thereof; ~~and~~

providing a reader for reading said smart card and including a database holding

information related to unauthorized smart cards, said reader being on-line, such that said

reader is operatively connected to a network, only when said database of said reader is being

updated by said network,

wherein said reader includes a random number generator, which, when a card

is read, chooses a pair (a, b) of distinct numbers with a < b between 1 and N,

wherein said smart card carries thereon predetermined N channels as C1,

C2,...., CN, where N is an integer,

wherein each channel C_i, with i equal to 1, 2, ..., N, carries a pair of numbers

(h_i, l_i), and

wherein h_i is the ith *high number* and l_i is the ith *low number*,

wherein said reader obtains a content of only two of said channels, and

periodically communicating, by said reader of said smart card, with a database where

a predetermined characteristic of the card is checked.

U.S. Application No. 09/685,026   3
Docket No. YOR920000165US1
(YOR.203)

2.   (Canceled).

3.   (Original) The method of claim 1, wherein an entire process of said method is

performable off-line.

4.   (Canceled).

5.   (Original) The method of claim 4, further comprising:

using public key cryptography with associated encoding and decoding functions Vi

and Vi^{-1} in each channel i,

wherein each function Vi^{-1} is known publicly, and Vi is known only to a

predetermined party representing an owner of the smart card.

6.   (Original) The method of claim 5, wherein for each i in 1, 2 ,..., N, the pair (hi, li) is

such that $hi = Vi(li)$, or $hi = Vi(K(li))$, where K represents a publicly-known cryptographic

hash function, and

wherein each li contains a plurality of symbols for redundancy.

7.   (Original) The method of claim 6, further comprising:

U.S. Application No. 09/685,026   4
Docket No. YOR920000165US1
(YOR.203)

processing, using an invertible function f which is made public, such that the low

numbers in said smart card satisfy $l(i+j) = f^j(li)$, where f^j represents the jth iteration of the

function f.

8.   (Previously presented) The method of claim 6, wherein before processing the smart

card, the reader obtains the pair (ha, la) and hb;

using the public keys Va^{-1} and Vb^{-1}, checking by the reader whether the pairs (ha, la)

and (hb, lb) are compatible, and, consequently, that the numbers ha, la, and hb belong to a

same legitimate card.

9-10.   (Canceled).

11.   (Original) The method of claim 10, wherein the predetermined characteristic

comprises whether a smart card has delivered more than a predetermined amount of money

to a user of the smart card.

12.   (Original) The method of claim 11, wherein if a card is detected as delivering too

much money, the data base communicates a corresponding number 11 to all readers in a

network, so that smart cards carrying said corresponding number are declined.

13.   (Original) The method of claim 1, wherein said cryptographic structure is changed

periodically.

U.S. Application No. 09/685,026   5
Docket No. YOR920000165US1
(YOR.203)

14.   (Original) The method of claim 1, wherein said smart card is invalidated after a

predetermined time of usage.

15.   (Original) The method of claim 8, wherein said pairs (hi, li) to be contained on the

smart card are generated by:

choosing a prefix of l1 once for all transactions, or changed whenever needed,

wherein said prefix is publicly known; and

providing a sequence, such that the sequence is generated so that a same number is

not chosen twice, and so that corresponding other li's are not chosen as new l1s.

16.   (Original) The method of claim 15, further comprising:

concatenating the prefix and the sequence to form l1; and

choosing a function f which is invertible and is publicly known, to construct $l2 = f(l1)$, $l3 = f(l2)$, and so forth.

17.   (Original) The method of claim 16, wherein the function f is chosen to be the identity

map, in which case $l1 = l2 = l3 = ... = lN$.

18.   (Original) The method of claim 17, choosing, for a number N, N public key-private

key pairs, such that a first private key V1 is for computing $h1 = V1(l1)$, a second private key

V2 is for computing $h2 = V2(l2)$, and so on.

U.S. Application No. 09/685,026   6
Docket No. YOR920000165US1
(YOR.203)

19.   (Original) The method of claim 18, further comprising:

verifying whether the smart card is authentic; and

checking whether the smart card is not in a list of cards to be refused.

20.   (Previously presented) The method of claim 1, wherein, when the smart card is read

by said reader, a random generator is prompted which provides two integer numbers, a and b,

which are not between 1 and N, with a < b.

21.   (Original) The method of claim 20, wherein said numbers a, b are transmitted to the

smart card which delivers two high numbers ha, hb, and a low number la in a channel a, and

wherein the pair (a, b), together with a function f in a memory in the reader, are used

to compute the low number $lb = f^{(b-a)}(la)$, said memory in said reader delivering public keys

Va^{-1} and Vb^{-1}.

22.   (Original) The method of claim 21, wherein the public keys are used by a comparator

together with the pairs (ha, la) and (hb, lb), to verify that the pairs are compatible with the

corresponding keys, and that the pairs are from a same legitimate card.

23.   (Previously presented) The method of claim 1, further comprising:

performing a final validation of the smart card by at least one of:

U.S. Application No. 09/685.026   7
Docket No. YOR920000165US1
(YOR.203)

        contacting a central data base if an entire transaction is made on-line with no

penalty; and

        checking with a local data base in said reader, said local database being

refreshed periodically by contact between said local database and said central database.

24.   (Previously presented) A method of preventing counterfeiting of a smart card,

comprising:

        providing a smart card such that none of confidential information and a cryptographic

key for authorizing the smart card, is carried on the smart card;

        reading said card by a reader such that in each reading, said reader reads only a

predetermined small amount of information which makes the card unique,

        wherein said reader includes a random number generator, which, when a card is read,

chooses a pair (a, b) of distinct numbers with a < b between 1 and N,

        wherein before processing the smart card, the reader obtains the pair (ha, la) and hb;

        using the public keys Va^{-1} and Vb^{-1}, checking by the reader whether the pairs (ha, la)

and (hb, lb) are compatible, and, consequently, that the numbers ha, la, and hb belong to a

same legitimate card.

25.   (Original) The method of claim 24, wherein a transaction performed under said

method comprises substantially an off-line transaction.

26.   (Previously presented) A system for preventing cloning of a smart card, comprising:

U.S. Application No. 09/685,026   8
Docket No. YOR920000165US1
(YOR.203)

a smart card such that a cryptographic structure for authorizing the smart card is not

carried on the smart card; and

a reader for reading the smart card and including a database for linking to a network

and being updated periodically with a list of unauthorized smart cards,

wherein said reader includes a random number generator, which, when a card is read,

chooses a pair (a, b) of distinct numbers with a < b between 1 and N,

wherein before processing the smart card, the reader obtains the pair (ha, la) and hb,

using the public keys Va^{-1} and Vb^{-1}, checking by the reader whether the pairs (ha, la)

and (hb, lb) are compatible, and, consequently, that the numbers ha, la, and hb belong to a

same legitimate card, and

wherein said cryptographic structure is kept secret by whoever emits the card or an

agent thereof.

27.   (Previously presented) A signal-bearing medium tangibly embodying a program of

machine-readable instructions executable by a digital processing apparatus to perform a

method for preventing counterfeiting and cloning of smart cards, comprising:

providing a smart card with a cryptographic structure for authorizing the smart card

which cannot be accessed completely by a predetermined number of readings,

reading said card by a reader such that in each reading, said reader reads only a

predetermined small amount of information which makes the card unique,

wherein said reader includes a random number generator, which, when a card is read,

chooses a pair (a, b) of distinct numbers with a < b between 1 and N,

U.S. Application No. 09/685,026   9
Docket No. YOR920000165US1
(YOR.203)

wherein before processing the smart card, the reader obtains the pair (ha, la) and hb;

using the public keys Va^{-1} and Vb^{-1}, checking by the reader whether the pairs (ha, la)

and (hb, lb) are compatible, and, consequently, that the numbers ha, la, and hb belong to a

same legitimate card, and

wherein said cryptographic structure can be built only by whoever emits the card or

an agent thereof.

28.   (Previously presented) The method of claim 1, wherein information stored on said

smart card is devoid of confidential information.